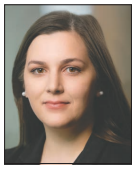
Data Security and Privacy in 2020 and Looking Ahead

By Anna Mercado Clark and Mary-Jane R. Morley
Phillips Lytle LLP

In 2020, individuals, organizations, regulators and courts faced unprecedented data challenges. COVID-19 required a quick transition to remote working and learning, brought on a rise in cyber incidents and put the spotlight on challenges relating to biometric technologies. Although legislative activity stalled, many laws were passed, enacted or went into effect in 2020, and significant developments continue to be expected in 2021.

Anna Mercado Clark
Partner



Mary-Jane R. Morley
Team Member

Statutory and Regulatory Developments

The past year saw increased regulatory and legislative activity. For example, the U.S. Securities and Exchange Commission (SEC) issued a cyber risk alert and initiated multiple enforcement actions regarding digital assets and cryptocurrency, while the U.S. Department of Health and Human Services' (HHS) Office for Civil Rights issued guidance and relaxed certain HIPAA requirements to cope with COVID-19 challenges. Moreover, despite stalled legislative activity, amendments to the California Consumer Privacy Act of 2018 (CCPA) were passed, and enforcement began on July 1, 2020, with related regulations taking effect in August 2020. California's Consumer Privacy Rights Act (CPRA), which expands the CCPA, also passed by referendum in November and is set to take effect in 2023. New York State's Stop Hacks and Improve Electronic Data Security Act (SHIELD Act), which requires, among other things, 'reasonable safeguards' to protect private data of New York State residents, also took effect in March. Privacy laws in Maine, Oregon and Texas also took effect (in some instances amending existing laws). Many of these laws seek to apply to organizations that are physically located outside of the governing state.

International Developments

From an international standpoint, Brazil's Lei Geral de Proteção de Dados (LGPD) came into effect, and Japan amended its Act on the Protection of Personal Information (APPI). Both laws mirror the European Economic Area's (EEA) General Data Protection Regulation (GDPR), including its extraterritorial reach, so that even organizations located solely in the United States may be subject to the laws. The GDPR continues to impact organizations' use and transfer of personal data, as well as individual enforcement of privacy rights. Significantly, in July, the Court of Justice of the European Union (CJEU) issued a decision in *Data Protection Commissioner v. Facebook Ireland Limited, Maximillian Schrems* (C-311/18) that invalidated the EU-U.S. Privacy Shield, which had been used by many U.S.-based organizations to transfer data from the EEA. It also called into question other commonly used data transfer mechanisms, such as standard contractual clauses. Invalidation of the Swiss-U.S. Privacy Shield followed shortly thereafter.

Looking Ahead to 2021

The data security and privacy landscape will continue to change in 2021, with the likely passage of stalled domestic privacy laws, enactment of international privacy legislation and continued challenges resulting from COVID-19. At the federal level, consideration of a comprehensive federal privacy act may gain momentum with the start of a new administration. New standard contractual clauses and additional guidance regarding cross-border data transfers between Europe and the U.S. are also expected. Heightened privacy concerns will continue as organizations work remotely and increasingly conduct business online. To safeguard against data security risks, organizations should continuously evaluate their current processes and policies to ensure compliance with relevant laws and regulations, and be prepared to adapt as the landscape evolves.

Anna Mercado Clark, CIPP/E, CIPP/US is a partner at Phillips Lytle LLP and leader of the firm's Data Security & Privacy and E-Discovery & Digital Forensics Practice Teams. She can be reached at aclark@phillipslytle.com or (716) 847-8400, ext. 6466.

Mary-Jane R. Morley is a member of Phillips Lytle LLP's Data Security & Privacy Practice Team. She can be reached at mmorley@phillipslytle.com or (716) 847-8348.